TECHNOLOGY ACCEPTABLE USE POLICY

Original Policy Date:	March 9, 2016
Revised Policy Date:	August 25, 2026
Issuing Office:	IT Department
Contact Information:	Manfred Krueger, Chief Information Officer

1.1 Purpose, Scope, and Definitions

1.1.1 Purpose

This Technology Acceptable Use Policy (AUP) governs the use of St. Francis College's IT Resources, including the College network, computing systems, applications, accounts, and information resources. The College provides IT Resources to support its academic mission, administrative operations, and research activities. Because these resources are shared and interconnected, the actions of a single User can affect the security, availability, and integrity of systems relied upon by the entire College community.

Use of IT Resources is a privilege, not a right. Access may be limited, suspended, or revoked at any time for improper use, at the direction of College leadership, or as required to protect the security or integrity of College systems. Use of IT Resources without authorization is prohibited, and any activity that prevents IT Resources from meeting their primary purpose may be terminated without notice.

1.1.2 Scope

This policy applies to:

1. All students, faculty, staff, administrators, temporary employees, contractors, vendors, volunteers, guests, and other affiliates who access or use College IT Resources.
2. All College-owned or College-managed devices, networks, systems, applications, and data, whether located on campus or accessed remotely.
3. All personally owned devices when connected to the College network or VPN, or when used to access any College system or account, including College-provided cloud services such as the College email and productivity suite.
4. Use of College IT Resources from any location, including residence halls, off-campus housing, remote work locations, and while traveling.

This policy applies in addition to, and does not replace, other College policies — including the Student Handbook (The CORD), the Faculty Statutes, the Employee Handbook, FERPA compliance procedures, and Human Resources policies — or any applicable federal, state, and

local law. All individuals who use or access College IT Resources are required to comply with this policy and with the College's codes of conduct.

1.1.3 Definitions

1. **IT Resources** — all College-owned or College-licensed computing, network, telecommunications, and information assets, including hardware, software, data, accounts, and cloud services.
2. **User** — any individual granted access to IT Resources, including students, faculty, staff, administrators, contractors, and guests.
3. **Credentials** — usernames, passwords, multi-factor authentication codes, tokens, certificates, or other information used to authenticate a User's identity.
4. **Confidential Information** — any data protected by law or College policy, including but not limited to education records (FERPA), personally identifiable information, financial data (GLBA), health records (HIPAA, where applicable), and payment card data (PCI DSS).
5. **Malicious Software** — viruses, worms, trojans, ransomware, spyware, keyloggers, and any other software designed to damage, disrupt, or gain unauthorized access to systems or data.

1.1.4 Applicable Law

This policy is adopted and administered in compliance with, and should be read in conjunction with, the following federal and New York State laws and regulations, as each may be amended from time to time:

1. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, and its implementing regulations at 34 C.F.R. Part 99;
2. Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801 et seq., and the FTC Safeguards Rule, 16 C.F.R. Part 314;
3. Digital Millennium Copyright Act (DMCA), 17 U.S.C. 512;
4. Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030;
5. Electronic Communications Privacy Act, including the Stored Communications Act, 18 U.S.C. 2701 et seq.;
6. Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. 794; Title III of the Americans with Disabilities Act, 42 U.S.C. 12181 et seq.;
7. New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), N.Y. Gen. Bus. Law 899-aa (breach notification) and 899-bb (data security protections);
8. New York Education Law 2-d (unauthorized release of personally identifiable student information);
9. New York Labor Law 201-i (prohibition on employer requests for access to personal accounts) and 203-d (protection of employee personal identifying information);
10. Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. Parts 160 and 164, to the extent applicable; and

11. Any other applicable federal, state, or local law, regulation, or binding contractual obligation relating to data privacy, information security, or technology use.

1.2 Policies

1.2.1 General Principles

1. IT Resources are provided to support the College's educational, research, and administrative mission. All other uses are secondary.
2. Incidental personal use is permitted provided it is lawful, does not violate this policy, does not interfere with College operations, and does not consume a disproportionate share of shared resources.
3. Users are accountable for all activity conducted under their accounts and Credentials. Any policy or security violation traced to a particular account or IT Resource will be attributed to the individual to whom that account or resource is assigned, regardless of whether that individual personally committed the violation.
4. Sharing accounts or Credentials is prohibited. This prohibition admits no exception for convenience, coursework, or coverage of job responsibilities; see Section 1.3.2.
5. Users must comply with software licensing terms, copyright law, export control regulations, and all applicable College policies when using IT Resources.

1.2.2 Copyright and Licensing

1. Software may not be copied without the owner's permission, unless such copying is permitted by copyright law or by the applicable license agreement.
2. Users will respect the privacy of information stored on College computer systems, regardless of to whom it belongs. Users agree not to acquire or modify information belonging to another person without the permission of the original owner. Information that has been acquired from another person remains the property of the original owner and may not be used, distributed, or modified without that owner's permission for any reason.
3. Acquiring a copy of another person's work in any form, with or without the owner's permission, and presenting it as one's own work is an act of plagiarism, is forbidden, and is subject to disciplinary action. Providing your own work to another individual knowing that they intend to present it as their original work is likewise strictly prohibited.
4. The number of simultaneous users of any piece of software will not exceed the number permitted by the copyright, purchase, or license agreement for that software.
5. IT Resources will not be used to violate copyright, trademark, or patent law. This includes the unauthorized copying, distribution, or use of copyrighted material through peer-to-peer file sharing.
6. Users of personally owned devices will not use College networking resources to acquire or distribute copyrighted works without authorization.

7. Users will not modify software or data without the consent of the creator or owner of that software or data.
8. Users will not reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of any software licensed to or provided by the College, except as expressly permitted by the applicable license agreement or by applicable law.
9. The College complies with the Digital Millennium Copyright Act (DMCA) of 1998 and will take appropriate disciplinary action against individuals who use IT Resources to infringe copyright. The College has designated an agent to receive notifications of claimed infringement pursuant to 17 U.S.C. 512(c)(2), and the name and contact information of the designated agent are available on the College's website and registered with the U.S. Copyright Office. The College maintains and enforces a policy providing for the termination, in appropriate circumstances, of the accounts of Users who are repeat infringers.

1.2.3 Data Access and Confidentiality

1. Access to College data is granted for the sole purpose of fulfilling assigned academic or work responsibilities. Accessing, modifying, or deleting any data in a manner inconsistent with those responsibilities is a serious matter and a violation of this policy.
2. Users will access and use Confidential Information only as needed to perform authorized job or academic duties, in accordance with the principle of least privilege.
3. Many of the College's records fall into more than one data category (for example, alumni, employee, and student). Inappropriate changes can negatively affect the data required by multiple College departments and may therefore cause serious disruptions.
4. Confidential Information will not be disclosed to individuals who do not have a legitimate need to know, and will not be used for personal, commercial, or other purposes.
5. Confidential Information will be stored only in College-approved and sanctioned systems and storage locations. It will not be stored on personal devices, personal cloud accounts, removable media, or unapproved third-party services except as authorized by the Department of Information Technology.
6. Data protected by federal or state law will be handled in accordance with the requirements of the applicable law and any related College procedures. Users who are unsure whether data is subject to such requirements should ask before accessing, sharing, or transferring it.
7. All contracts with third-party vendors, contractors, and service providers who receive access to Confidential Information, including student data, shall contain provisions requiring those parties to maintain the security and confidentiality of such information in accordance with applicable federal and state law, including but not limited to FERPA, GLBA, and NY Education Law 2-d.

8. Any suspected or actual data breach, unauthorized disclosure, or loss of Confidential Information must be reported immediately in accordance with Section 1.2.13.
9. Questions relating to the appropriate use of access to College data should be discussed with the User's immediate supervisor, the Department of Information Technology, and/or the Office of Human Resources.

1.2.4 Authentication and Account Security

1. Passwords for College accounts must be at least eight characters long and must contain at least one uppercase letter, at least one number, and at least one special character. A password must not contain the User's name. A College network account password must not be reused on any non-College site or service.
2. Passwords must be changed at least every 90 days on all College systems.
3. Users must enroll in and use multi-factor authentication (MFA) where the College has made it available, and must never approve an MFA prompt that was not initiated by their own login attempt.
4. Credentials are the first line of defense for protecting College accounts and College data. Users must never share passwords, MFA codes, security tokens, or other Credentials with anyone, including IT staff, supervisors, faculty, classmates, colleagues, or family members. The Department of Information Technology will never ask a User for a password.
5. Users will only use accounts assigned to them. Accessing someone else's account, or providing someone else with access to your account, is prohibited and subject to disciplinary action.
6. Users must lock or log off any device before leaving it unattended, and must enable automatic screen locking on all devices used to access College systems. Although College computer systems are set to lock after a period of inactivity, Users should not rely on that mechanism alone.
7. Suspected compromise of Credentials — following a phishing attempt, a lost device, or suspicious account activity — must be reported immediately in accordance with Section 1.2.13.

1.2.5 Network Access and Connected Devices

1. Users will not connect unauthorized routers, switches, wireless access points, hubs, or other network infrastructure devices to the College network without prior written approval from the Department of Information Technology.
2. Users will not extend the College network by means of personal Wi-Fi hotspots, bridging software, or similar methods in ways that bypass network security controls.
3. Personal and Internet-of-Things devices, such as smart televisions, gaming consoles, and smart-home devices, may connect only to network segments designated for such devices.

4. Users must use the College-provided VPN for remote access to internal, non-public College systems, and must not use unauthorized remote access tools, such as unmanaged remote desktop software, to connect to College systems.
5. Users will not attempt to circumvent network security controls, including firewalls, content filters, network segmentation, or intrusion prevention systems.
6. The use of personal computers and devices is otherwise permitted on the College network; owners remain responsible for the maintenance and support of those systems.
7. Only IP addresses assigned by the Department of Information Technology may be used on the College network, and all devices that access the College network must be registered with the Department where registration is required.

1.2.6 Malicious Software and System Integrity

1. Users must keep operating systems, applications, and anti-malware software current, supported, and enabled on any device used to access IT Resources.
2. Users will not disable, tamper with, or attempt to bypass College-managed security software, including endpoint protection, disk encryption, and patch management agents, on College-owned devices.
3. Users will not knowingly introduce Malicious Software onto College systems or networks, and must exercise caution with email attachments, downloads, and removable media from unknown or untrusted sources.
4. Users will not install unauthorized or unlicensed software on College-owned devices.
5. Suspected malware infections, ransomware indicators, or unusual system behavior must be reported immediately in accordance with Section 1.2.13, and the affected device disconnected from the network if instructed to do so.

1.2.7 Scanning, Testing, and Unauthorized Access

1. Users will not perform network scans, vulnerability scans, penetration testing, or port scanning against College or third-party systems without prior written authorization from the Department of Information Technology.
2. Users will not attempt to access accounts, data, systems, or network segments for which they have not been granted explicit authorization, regardless of whether a technical vulnerability makes such access possible, and whether the system is on or off campus.
3. Users will not intercept, monitor, or capture network traffic, including by packet sniffing, except where required for authorized administrative duties. Users will not install software or hardware that monitors keyboard activity, internet access, or other user activity on IT Resources, including traffic sniffers, key loggers, and other data logging applications configured to violate an individual's privacy.
4. Users will not use IT Resources to attack other resources or individuals, to conduct denial-of-service attacks, to spoof network identities, or otherwise to disrupt the

availability of College or third-party systems. Users will not use IT Resources to spread spam, chain email, phishing messages, or hoaxes, or to relay unsolicited bulk email on behalf of third parties. Performing these activities will be grounds to have all access terminated.

1.2.8 Encryption and Data Protection

1. Users must use only College-approved, encrypted methods — the College VPN, secure file-transfer tools, or encrypted email — to transmit Confidential Information.
2. Users will not transmit Confidential Information over unencrypted channels, personal email accounts, or unapproved cloud storage and file-sharing services.
3. Confidential Information stored on College systems or devices must be encrypted at rest using College-approved encryption methods. Users must not store Confidential Information on any system, device, or medium that does not support encryption at rest, unless an exception has been approved in writing by the Department of Information Technology.
4. Users must exercise heightened caution on public or unsecured Wi-Fi networks and must use the College VPN when accessing College systems from such networks.

1.2.9 Personal Devices

1. Personal devices used to access College email, systems, or Confidential Information must meet minimum security requirements, including a screen lock, a current and supported operating system, and active anti-malware protection where applicable.
2. The College may require enrollment of a personal device in a mobile device management solution when that device is used to access certain Confidential Information or systems. The College reserves the right to remotely remove College data — but not personal data — from such devices upon loss, theft, or termination of affiliation.
3. Users are responsible for promptly reporting the loss or theft of any personal device that has been used to access IT Resources.

1.2.10 Email, Messaging, and Communication Tools

1. College email and messaging systems are the official channel for College business communications and must be used in a manner consistent with this policy.
2. Users must exercise caution with unsolicited email, attachments, and links, and should report suspected phishing messages through the College's designated reporting mechanism rather than clicking on or responding to them.
3. Automatic forwarding of College email to a personal or non-College email account is prohibited unless approved in writing by the Department of Information Technology.
4. Users identifying themselves as affiliated with the College on social media or other public platforms should exercise good judgment and are personally responsible for the content they post. *See* Social Media Policy (last revised Aug. 23, 2024).

1.2.11 General Usage

1. IT Resources are shared resources, and all Users are expected to keep their use of these resources to a reasonable level. Access may be denied to any User found to be taking unfair advantage of these shared offerings or engaging in personal use that degrades network performance or availability for others.
2. Users engaged in educational or work activities have priority over anyone using those resources for recreational activity. A User who needs a particular resource may ask a recreational user of that resource to stop if there are insufficient resources available for educational or work activity.
3. Use of internet communication is voluntary, with the understanding that Users may encounter material they find offensive. St. Francis College assumes no responsibility for the material viewed.
4. Users will not violate federal, state, or local law through IT Resources, including copyright, export control, and computer fraud statutes.
5. Users will not access, store, or distribute illegal content through IT Resources.
6. Harassment, threats, defamation, or discriminatory conduct directed at any member of the College community through IT Resources is prohibited. Users will not commit fraud or identity theft, or misrepresent their identity, when using IT Resources.
7. The use of IT Resources for unauthorized commercial purposes, personal financial gain, or outside employment not sanctioned by the College is forbidden.
8. The College reserves the right to require the removal of any technology resource deemed a security or network risk.
9. Users waive any right to compensation for lost work or time due to issues with IT Resources.
10. All Users agree not to take any actions that would be considered inappropriate. Such actions may include, but are not limited to, harassment, foul or abusive language, consumption of food or drink in computer labs, or any other behavior that causes distractions to others.

1.2.12 Theft and Damage

1. Theft, rearrangement, or damage to College technology assets is forbidden.
2. Anyone using the technology assets of the College agrees to use those resources in a careful and responsible manner.
3. Users are financially responsible for the loss, damage, or destruction of equipment caused by negligence, misuse, abuse, or carelessness.
4. Any equipment that is stolen, whether personally owned or College owned, should be reported to the Office of Safety and Security and to the Department of Information Technology.

1.2.13 Incident Reporting

Users must promptly report any of the following to the Service Desk:

1. Suspected phishing, social engineering, or fraudulent communications.
2. Suspected or confirmed Malicious Software, ransomware, or unauthorized system access.
3. Lost or stolen devices that have accessed IT Resources or College data.
4. Suspected compromise of Credentials or unusual account activity.
5. Any suspected data breach or unauthorized disclosure of Confidential Information.

Reports may be made to the St. Francis College Service Desk at servicedesk@sfc.edu or (718) 489-5444.

In the event of a confirmed breach of the security of the system, the College will notify affected individuals as soon as reasonably possible after discovery of the breach. The College will comply with all notification requirements under applicable federal, state, and local law. All breach notifications will include the categories of information affected and contact information for the College and for relevant state and federal agencies.

Reporting a security concern in good faith will not result in disciplinary action against the reporting individual, even where the report reveals that the individual's own account or device was involved, provided the individual has not otherwise violated this policy. Failure to report a violation of this policy will itself be treated as a violation.

1.2.14 System Administrator Responsibilities

1. System administrators will monitor IT Resources for their availability.
2. College administrators will develop policies and implement technologies to prevent theft of or damage to IT Resources.
3. System administrators are responsible for securing central technology resources used by members of the College community.
4. System administrators will follow and enforce the agreements governing the software and hardware packages that they maintain.
5. System administrators will cooperate with administrators or legal entities from off-campus locations to address problems caused by IT Resources.
6. System administrators will enforce the policies created by St. Francis College that govern the operation of the College and its assets.
7. System administrators will not access or view a personally owned computer without the consent of the owner.

The Chief Information Officer, or a designee, shall serve as the College's designated coordinator for its information security program.

The [Chief Information Officer/Department of Information Technology] will conduct periodic risk assessments to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Confidential Information, and will assess the sufficiency of safeguards in place to control identified risks.

The Department of Information Technology will maintain and periodically test an incident response plan addressing the College's procedures for responding to security incidents and data breaches.

The Chief Information Officer [or other designated coordinator of the College's information security program] shall report in writing, at least annually, to the College's Board of Trustees or equivalent governing body on the overall status of the information security program and its compliance with applicable requirements, including material matters related to risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

1.2.15 Monitoring and Privacy

Users should have no expectation of complete privacy when using College IT Resources.

1. The College reserves the right to monitor, log, and review network traffic, system activity, and account usage for security, performance, legal, and policy-compliance purposes, consistent with applicable law.
2. The College may access, review, or disclose the contents of College accounts and systems when necessary to investigate a suspected policy violation, respond to legal process, ensure business continuity, or protect the health and safety of the community, subject to authorization by appropriate College officials.
3. Automated security tools — including anti-malware, intrusion detection and prevention, data-loss prevention, and spam and phishing filtering — operate continuously on IT Resources as a routine security measure.

Any such monitoring, and any resulting access to account content, will be conducted in accordance with the College's governance procedures and applicable law, and will be limited to legitimate business, academic, or security purposes. Nothing in this policy authorizes the College to require an employee to disclose access credentials to a personal account, or to access an employee's personal account.

1.2.16 Accessibility and Accommodations

1. Users who require accommodations or modifications to access IT Resources due to a disability should contact the College's Office of Accessibility & Accommodations. . The College's General Accessibility and Accommodation's policy can be found at General-Accommodations-Procedure-12.19.2024.pdf .

2. Requests for accommodations related to IT Resources will be evaluated by the Office of Accessibility & Accommodations in consultation with the Department of Information Technology, not through the general policy exception process described in Section 1.5.

3. Concerns about inaccessible IT Resources may be reported to the Department of Information Technology or to the Office of Accessibility & Accommodations.

4. The College's General Accessibility and Accommodation's policy can be found at General-Accommodations-Procedure-12.19.2024.pdf.

1.2.17 Artificial Intelligence

1. Generative artificial intelligence tools, AI-assisted writing and research tools, and other AI-enabled services (collectively, "AI Tools") may be used in connection with IT Resources only in accordance with this section and any supplemental College policies or faculty guidelines on AI use:

2. Users must not input Confidential Information, including student education records, personally identifiable information, financial data, or health records, into any AI Tool that has not been approved by the Department of Information Technology for use with such data.

3. Students must follow all course-specific guidelines established by their instructors regarding the permissible use of AI Tools for academic work. Presenting AI-generated content as one's own original work without proper attribution, where such use has not been authorized by the instructor, may constitute a violation of the College's academic integrity policies.

    a. The Department of Information Technology will maintain and publish a list of AI Tools that have been reviewed and approved for use with College data. Users should consult that list before using AI Tools in connection with College IT Resources or data.

4. Users must exercise professional judgment when relying on AI-generated output and should verify the accuracy of any such output before using it for College business, academic, or administrative purposes.

1.2.18 Data Retention and Disposal

The College will maintain Confidential Information only for so long as there is a legitimate business, academic, or legal need to do so, consistent with applicable records retention schedules and legal requirements. When Confidential Information is no longer needed for business or legal purposes, it will be disposed of in a manner that renders it unreadable and unrecoverable, including

by securely erasing electronic media so that the information cannot be read or reconstructed. Users must not retain Confidential Information beyond its approved retention period or store it in locations not sanctioned by the Department of Information Technology. Disposal of physical media containing Confidential Information must be conducted through approved methods such as shredding, degaussing, or physical destruction.

1.2.19 Training and Awareness

The College will provide periodic security awareness training to all Users who access or handle Confidential Information. Training will address, at a minimum, the requirements of this policy, phishing and social engineering awareness, proper handling of Confidential Information, incident reporting procedures, and the applicable legal requirements governing data privacy and security. New Users will receive training as part of their onboarding process. The Department of Information Technology will maintain records of training completion. Users who fail to complete required training within designated timeframes may have their access to IT Resources restricted until training is complete.

1.2.20 Student Identity Verification for Distance Education

The College employs processes to verify that a student who registers for a distance education or online course is the same student who participates in and completes the course. These processes include the assignment of unique Credentials upon admission, mandatory enrollment in multi-factor authentication (MFA) at first login, and the prohibition on sharing Credentials set forth in this policy. Students enrolled in distance education courses are notified at the time of registration if any projected additional charges are associated with student identity verification. The College's identity verification processes are designed to protect student privacy in accordance with FERPA.

1.3 Account Locks, Misuse, and Consequences

The Department of Information Technology distinguishes between an account that has been locked because a third party gained access to it unlawfully or without the permission of the account holder, and an account that has been locked because the account holder did something they were not permitted to do.

1.3.1 Security Locks

A security lock is an account lock imposed for any reason other than misuse by the account holder. Security locks include, but are not limited to, locks imposed because:

- a third party has gained access to the account without the account holder's authorization, whether by phishing, credential theft, malware, session hijacking, or any other means;
- the account holder was the target of an attack rather than its source;
- of failed login attempts, password expiry, or automated detection of anomalous activity; or
- of routine administrative maintenance.

A security lock is a security incident, and not a disciplinary matter. It carries no consequences under this section and does not count toward the sequence described in Section 1.3.4. Section 1.2.13 requires account holders to report a suspected compromise immediately, and no account holder will be penalized under this policy for making such a report in good faith.

1.3.2 Misuse and Policy Violation Locks

Misuse means conduct by the account holder that violates any Section of this policy and that the account holder undertook knowingly. Misuse does not require malicious intent or any intent to cause harm. Conduct undertaken for a convenient, well-meaning, academic, or work-related reason is still misuse if the account holder knew, or reasonably should have known, that it was prohibited. Misuse includes, but is not limited to:

- sharing Credentials with another person, or using Credentials assigned to another person, for any reason — including to complete or submit coursework, to allow a classmate or colleague to access a system on one's behalf, to cover job responsibilities during an absence, or to work around a delay in obtaining one's own access;
- accessing, modifying, or deleting College data outside the scope of one's assigned responsibilities;
- circumventing, disabling, or declining to maintain a required security control;
- using IT Resources to attack, harass, or impersonate others, or for commercial purposes or personal financial gain.

A policy violation lock is an account lock imposed in response to misuse. Only policy violation locks carry the consequences described in Sections 1.3.4 through 1.3.6.

1.3.3 Determining the Type of Lock

The Department of Information Technology will classify each account lock as either a security lock or a policy violation lock. Where the correct classification is not yet clear, the lock will be treated as a security lock until the review is complete.

A lock initially classified as a security lock may be reclassified as a policy violation lock if the review establishes that the unauthorized access was made possible by the account holder's own violation of this policy — for example, by sharing Credentials with another person, or by circumventing a required security control. An account holder who was deceived by a phishing message or other attack has not, by that fact alone, committed misuse.

1.3.4 Consequences for Students

The following graduated consequences apply to students. A policy violation lock counts toward this sequence for 24 months from the date it is imposed; earlier locks are disregarded.

1. **First Lock:** Upon a first policy violation lock, the account holder must contact the Service Desk to review the circumstances of the violation. The account will be reinstated

once the account holder has presented government-issued identification, either in person or by video, and staff have confirmed that the issue has been addressed.

2. **Second Lock:** A second policy violation lock requires the account holder to complete a formal review with the Department of Information Technology covering this policy and the College's requirements for the appropriate use of IT Resources. The account will remain locked until that review has been completed, the account holder has again presented government-issued identification, either in person or by video, and the account holder has acknowledged the applicable policies.
3. **Third Lock:** A third policy violation lock will be referred to the Office of the Dean for disciplinary action pursuant to the provisions of the Student Handbook. The account will remain suspended pending the outcome of that referral, and the Dean's Office will determine appropriate corrective action.

1.3.5 Consequences for Faculty, Staff, and Administrators

A policy violation lock involving a member of the faculty, staff, or administration will be referred to the Office of Human Resources upon the first occurrence. The account will remain locked pending the outcome of that referral, and the timing of reinstatement will be determined by the Department of Information Technology in consultation with the Office of Human Resources. Any resulting disciplinary action will be taken in accordance with the applicable College handbook and any governing collective bargaining agreement.

1.3.6 Other Authorized Users

For guests, contractors, vendors, volunteers, and other authorized Users who are not students or employees of the College, a policy violation lock may result in the suspension or revocation of access, and the matter will be referred to the sponsoring College department.

1.3.7 Immediate Suspension and Acceleration

The Department of Information Technology may immediately suspend network or system access, without prior notice, where necessary to protect the security or integrity of IT Resources or the broader community, pending investigation. Such a suspension is not itself a determination that misuse occurred.

The College reserves the right to accelerate the process described in this section, at any step and for any category of User, in cases involving serious or willful misuse of College systems or data.

1.4 Violations

A violation of this policy may result in disciplinary or punitive action in addition to the policy violation locks described in Section 1.3. Such action may include, but is not limited to, suspension of technology privileges, revocation of technology privileges, charges and/or fines for damages incurred, suspension from the College or from employment by the College, expulsion from the College or termination of employment with the College, and referral to local, state, or federal law

enforcement agencies. A violation may also result in civil or criminal liability under applicable law.

Disciplinary determinations will be made through the appropriate College process, with due process protections as applicable. Disciplinary action involving employees will be taken in accordance with the Faculty Statutes, applicable College handbook, and any governing collective bargaining agreement. Any decision made in regard to a violation of this policy may be appealed through the proper channels.

1.5 Exceptions

Any exception to this policy — for example, for authorized security testing or research requiring specialized network configurations — must be requested in writing and approved in advance by the Chief Information Officer or designee. Exceptions will be documented, time-limited where appropriate, and subject to periodic review. Requests for disability-related accommodations are not subject to this exception process and will instead be handled through the College's Office of Accessibility & Accommodations as described in Section 1.2.16.

1.6 About this Policy

This Technology Acceptable Use Policy will remain in effect for as long as an individual makes use of St. Francis College IT Resources. The Department of Information Technology will review this policy at least annually and may add rules, regulations, or guidelines related to the acceptable use of IT Resources. The policy will be updated as necessary to reflect changes in applicable law, technology, or institutional operations. A current copy of this policy can be found at www.sfc.edu.

1.7 Contact

If a violation of this policy or of other College technology policies occurs, individuals should report it to the Service Desk at servicedesk@sfc.edu or (718) 489-5444. Failure to report a violation of this policy will be treated as a violation. For questions or clarification regarding this policy, please contact Manfred Krueger, Chief Information Officer. The Department of Information Technology reserves the right to update this Acceptable Use Policy when it is deemed necessary.

1.8 Disclaimer of Warranties and Limitation of Liability

IT Resources are provided on an "as is" and "as available" basis. The College makes no warranties, express or implied, regarding the reliability, availability, suitability, security, or accuracy of IT Resources, and expressly disclaims any warranty of merchantability or fitness for a particular purpose. The College shall not be liable for any direct, indirect, incidental, special, or consequential damages arising out of or in connection with the use of, or inability to use, IT Resources, including but not limited to loss of data, loss of work product, interruption of service, or damages resulting from unauthorized access to or alteration of User transmissions or data. The College is not responsible for the content of any information transmitted or received through IT

Resources. Users assume full responsibility for any reliance placed on IT Resources and for backing up their own data.

1.9 User Acknowledgment

All Users are required to acknowledge that they have read, understand, and agree to comply with this Technology Acceptable Use Policy as a condition of receiving or maintaining access to College IT Resources. For employees, acknowledgment will be obtained upon hire and annually thereafter. For students, acknowledgment will be obtained at the time of initial enrollment. For contractors, vendors, guests, and other authorized Users, acknowledgment will be obtained prior to receiving access. Failure to provide acknowledgment does not relieve a User of the obligation to comply with this policy.